



## Retos en Ciberseguridad y Riesgos Tecnológicos

**MODALIDAD**  
Teleformación

**Nº DE HORAS**  
30 horas

**NIVEL**  
Iniciación

### Objetivos

El curso tiene como objetivo proporcionar a los alumnos una comprensión integral de la gestión de riesgos en los sistemas de información. A través del análisis y la identificación de riesgos, los participantes aprenderán a evaluar y tratar amenazas de manera efectiva utilizando métodos cualitativos y cuantitativos, y familiarizarse con herramientas y normativas internacionales como ISO 31000 y ISO 27001. Además, se les capacitará en la planificación y respuesta a incidentes, garantizando la continuidad del negocio y la recuperación ante desastres.

Al finalizar el curso, los alumnos estarán preparados para implementar planes de gestión de riesgos en sus organizaciones, monitorizar y revisar continuamente estos riesgos, y aplicar buenas prácticas y estrategias de mitigación. Los conocimientos adquiridos les permitirán enfrentar desafíos reales de ciberseguridad y asegurar el cumplimiento regulatorio.

### Conocimientos previos y requisitos técnicos

Para aprovechar el curso de " Retos en Ciberseguridad y Riesgos Tecnológicos", los alumnos deberían tener conocimientos básicos de seguridad informática, fundamentos de redes y sistemas operativos. También es útil estar familiarizado con normativas y regulaciones de seguridad de la información y tener habilidades analíticas para evaluar riesgos.

Estos conocimientos previos garantizarán que los alumnos puedan seguir el curso de manera efectiva y aplicar de manera práctica las habilidades adquiridas. Esto les permitirá implementar estrategias de gestión de riesgos y asegurar el cumplimiento normativo en sus organizaciones.

### Metodología

La teleformación se basa en la flexibilidad y accesibilidad, permitiendo a los alumnos aprender a su propio ritmo desde cualquier ubicación. Utiliza plataformas en línea donde los estudiantes acceden a materiales del curso, contenido multimedia



interactivo, y participan en webinars y sesiones en vivo. Además, se realizan evaluaciones periódicas y se ofrece retroalimentación constante de los instructores y compañeros.

## Temario / Programa

### Introducción a la Gestión de Riesgos

- Conceptos básicos de gestión de riesgos
- Importancia de la gestión de riesgos en los sistemas de información
- Principios y terminología

### Identificación de Riesgos

- Técnicas y métodos de identificación de riesgos
- Análisis de amenazas y vulnerabilidades
- Evaluación del impacto potencial

### Análisis de Riesgos

- Evaluación cualitativa y cuantitativa de riesgos
- Métodos de análisis como OCTAVE, ISO 27005, y NIST
- Herramientas de análisis de riesgos

### Evaluación y Tratamiento de Riesgos

- Criterios de evaluación y aceptación de riesgos
- Estrategias de tratamiento de riesgos: mitigación, transferencia, aceptación, y evitación
- Desarrollo de planes de tratamiento de riesgos

### Monitorización y Revisión de Riesgos

- Procedimientos de monitorización continua
- Revisión y actualización periódica del análisis de riesgos
- Indicadores clave de riesgo (KRI)

### Gestión de Incidentes y Continuidad del Negocio

- Planificación de la respuesta a incidentes
- Estrategias de continuidad del negocio y recuperación ante desastres
- Integración de la gestión de riesgos con la gestión de incidentes

### Normativas y Estándares en Gestión de Riesgos



**TESLA**  
TECHNOLOGIES

**Tesla Technologies & Software, S.L.**

CIF: B-70.305.578

C/Fontiñas, nº 92

15703 – Santiago de Compostela

A Coruña (España)

- Principales normativas y estándares internacionales (ISO 31000, ISO 27001)
- Cumplimiento regulatorio y buenas prácticas

#### Casos Prácticos y Ejemplos Reales

- Análisis de casos de estudios
- Ejemplos prácticos de gestión de riesgos en organizaciones

#### Proyecto Final

- Desarrollo de un proyecto final

## Calendario

Fechas: Desde el 3 de febrero a 27 de marzo